RESEARCH PAPER

CYBER-DEFENSE OF DELHI SLDC

Abhay Pratap Singh | Microsoft Cybersecurity Engage | Indian Institute of Technology, Jodhpur | 22 June, 2022

ABSTRACT

This research paper addresses concerns of **National Critical Information Infrastructure Protection Centre (NCIIPC)** which is an organization of the Government of India and is responsible for protecting India's Critical Infrastructure like Power & Energy, Banking, Financial Services & Insurance, Telecom, Transport, Government Strategic & Public Enterprises.

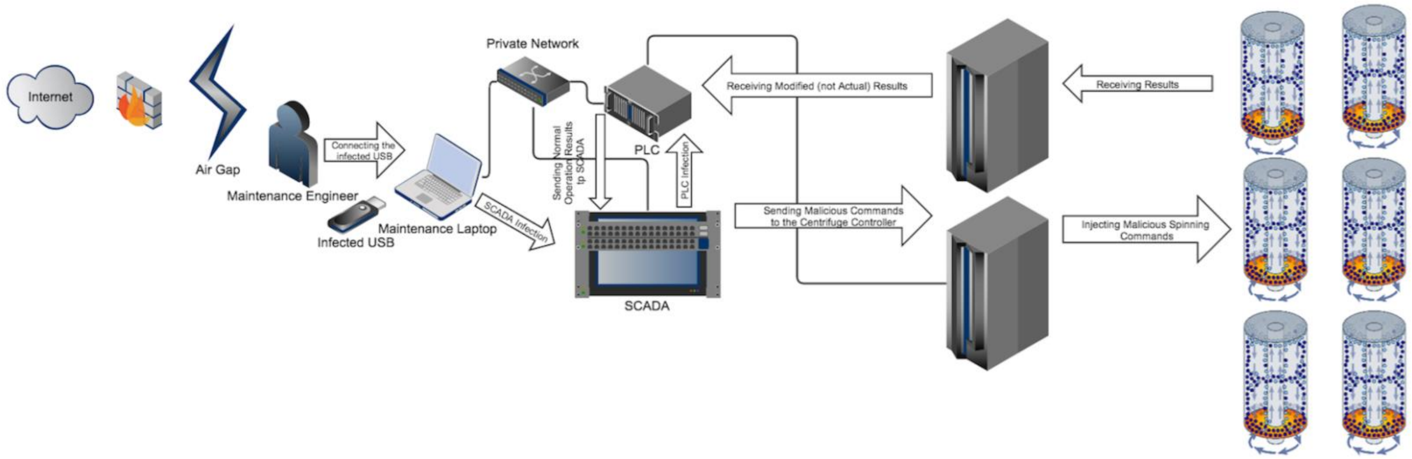
We look at the background of the scenario with Stuxnet and its implications on the *'Grey-zone'* warfare between nation states. We also list the reasons to prioritize the defense of one of the most important critical infrastructures in the country, ***Delhi State Load Dispatch Centre*** (SLDC) and the cyber-deterrence challenges we face in this regard.

I have proposed the solution architecture that constitutes of many ***techniques*** and ***processes*** at *physical, network and framework* levels to counter Stuxnet like cyber-attack or as often called 'Sons of Stuxnet'. I have tried my best to define the benchmarks for success, as in what constitutes a successful defense in this regard. Also, I have not only deep-dived into the technical solutions, processes, and frameworks, but also into the legal implications and possible courses of action.

BACKGROUND

Traditionally, prior cyber "attacks" had stayed within the digital realm, usually involving the theft, disruption, or manipulation of information. **Stuxnet** (which was developed and deployed as part of ***"Operation Olympic Games"*** to target Iran's Nuclear program) did that, but caused something new, and that's physical consequences. This made it like prior weapons in general, as all weapons throughout history had caused physical damage.

Stuxnet was exploiting several unknown "zero-day" vulnerabilities in the systems it hit and using fraudulent digital certificates to trick the systems into running its code. As it spread, it had to examine the hardware, software, and settings of each system to determine if they matched those at Natanz which was a specific type of program used in Siemens's WinCC/PCS 7 SCADA control software. If this software was not present, the worm had built-in controls to become inert. And when it did find the right system, it tampered with the code of the Programmable Logic Controller (PLC) used to control the IR-1 centrifuges at Natanz, ultimately destroying about a thousand centrifuges and disrupting Iran's nuclear program. [1] [2]

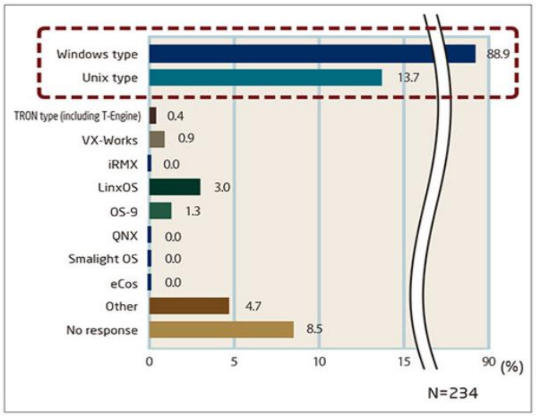

Internet
Air Gap
Maintenance Engineer
Connecting the infected USB
Infected USB
Maintenance Laptop
SCADA Infection
Private Network
Sending Normal Operation Results tp SCADA
PLC
PLC Infection
SCADA
Receiving Modified (not Actual) Results
Sending Malicious Commands to the Centrifuge Controller
Receiving Results
Injecting Malicious Spinning Commands

Moreover, it was extremely sophisticated in the approach, for example, The attack didn't shut down the centrifuges in any obvious manner. Instead, it ran a series of subroutines, for ex., caused tiny adjustments in the pressure inside the centrifuges (Man in the Middle Attack), manipulated the speed of the centrifuges' spinning rotors, causing them to first slow down, then return to normal speed, destabilizing the rotors and ruining their work, or sometimes push the centrifuge speeds past the designed maximum. All this while concealing its presence by behaving as a rootkit.

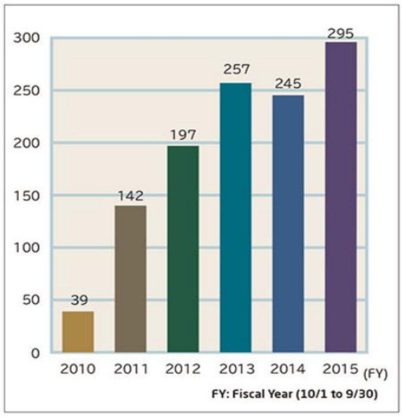
As a result, the centrifuges not only failed to produce refined uranium fuel, they frequently broke down and ground to a halt from the damaging vibrations caused by the virus and the scientists had no idea why. Also, with respect to command and control, Stuxnet needed to operate autonomously, with its commands and data wired into the code, although it also had the capability to receive new code over the Internet if so connected. [1][3]

This level of sophistication could only be achieved by large fundings and resources both in manpower and others. But Cyber weapons are no longer the exclusive purview of nation-states, though still they are certainly the major players. In the words of the renowned cryptographer Bruce Schneier, "-Today's NSA secrets become tomorrow's PhD -theses and the next day's hacker tools". [4]

Today, determined adversaries can purchase Stuxnet for a fraction of what it cost to develop and use the source code as a template. Experts agree that this is perhaps the most troubling consequence of Stuxnet—-the fact that its code can now be dissected and repurposed into new, possibly more dangerous weapons, weapons that can be used by cyber-terrorists as well. The attacks on a country's Critical Infrastructure are on an upwards trend since the public disclosure of Stuxnet malware in 2010 as shown below. [5]



OS usage (terminals) at industrial plants



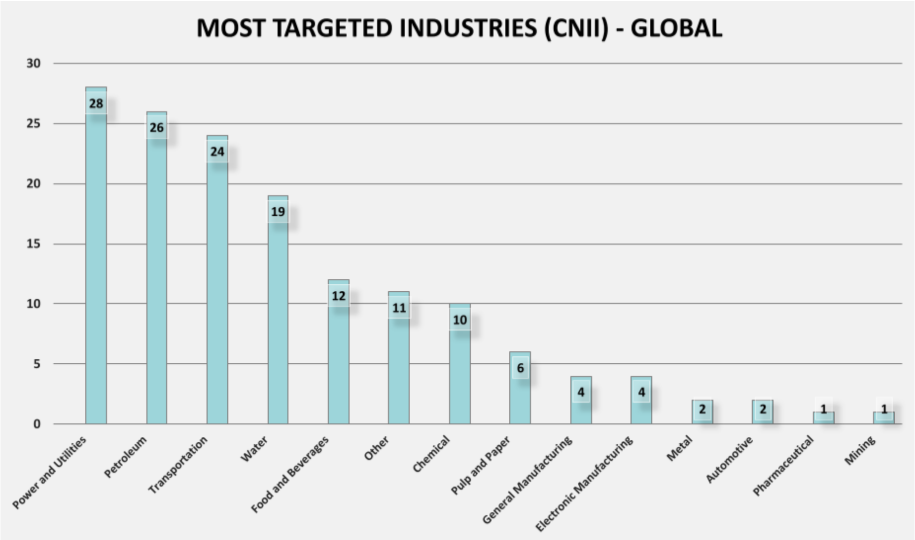
The number of cyber incidents responses by U.S. ICS-CERT

Now, malware has become a weapon in a nation's arsenal in 5th generation warfare. This has led to an arms race and escalation in cyber warfare, and Stuxnet will go down in history as "The keystroke heard around the world".

MOTIVATION TO PROTECT DELHI SLDC

As we have seen that nation states are capable of highly sophisticated cyber-attacks, this is part of grey-zone warfare that carries far less risks and little to no international accountability or in military terms strategic deniability.

Critical Infrastructure's definition as defined by NCIIPC is given above, but its role in nation's economy and general well-being is unparalleled and if such infrastructure is to be destroyed in kinetic action, it will constitute nothing less than full-scale war. But in event of a cyber-attack, hostile nations get the freedom to deny actions in cyber domains, which has led to scores of attacks on different kinds of CI as listed below. Arguably the most affected area of a nation's CI is Power sector. [6]



Source [6]

India has also been a victim of such campaigns for a long time, listing major cyber incidents from CSIS report on **"Significant Cyber Incidents Since 2006"** [7] have **60** incidents that took part on the Indian soil since 2006. The majority cyber-threats to Indian Critical Infrastructure comes from China and Pakistan, and some terrorist groups.

Though the government is also continuously under attack by cyber-activists and cyber-espionage attempts, but these are more focused on the data theft, etc. and don't aim to physically harm India's Critical Infrastructure.

We had deteriorating relations with China since Galwan Valley incident, below is given two parallel timelines from RecordedFuture report. The timelines are of Geopolitical or Military instances, and ThreatListMembershipAddition of C2 server , as shown in the legend in the reference shown below. [8]

We can observe that the Threat list starts growing at an alarming pace as the tensions started rising, these C2 were used to attack multiple critical infrastructures in India.

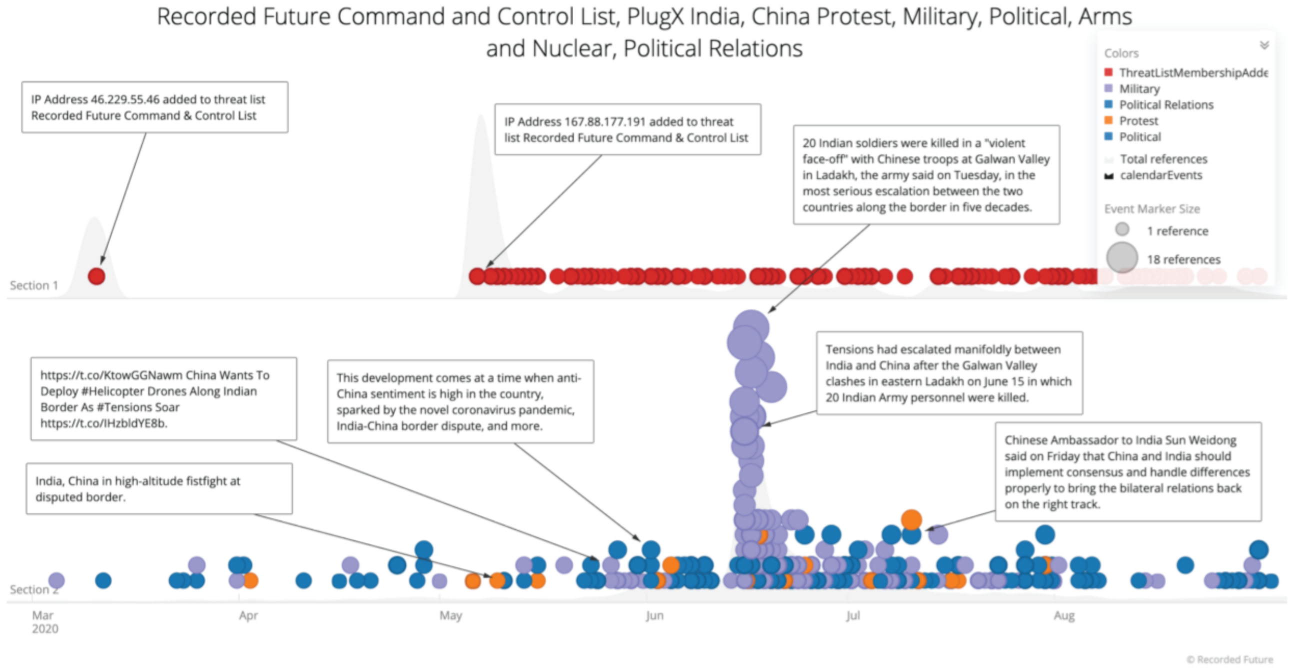
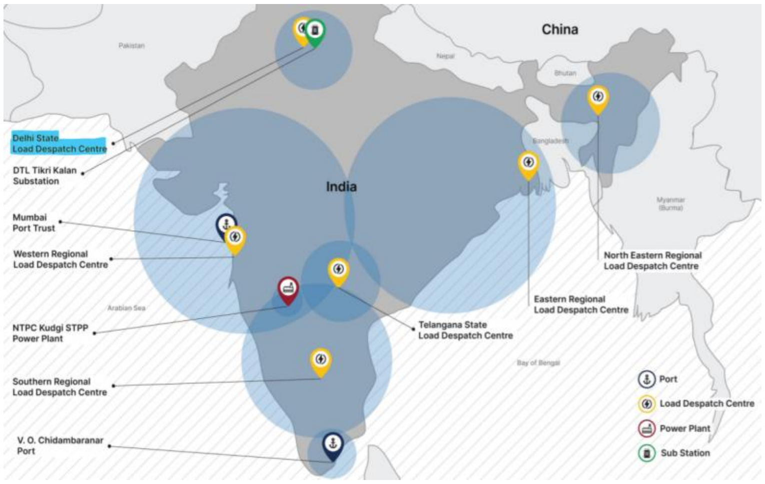
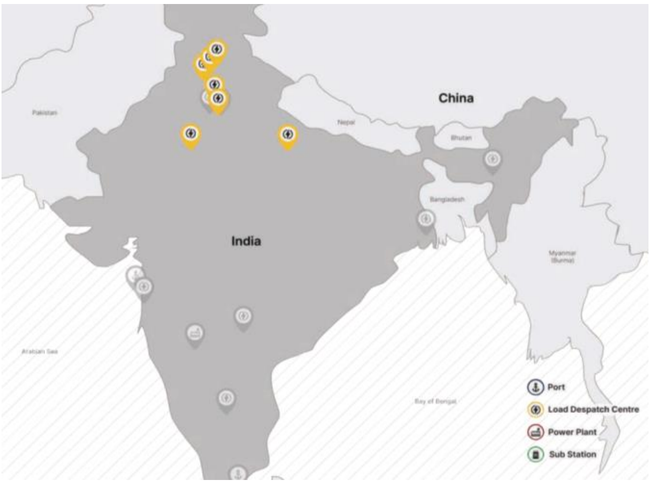


Figure 3: Timeline of Recorded Future PlugX C2 detections aligned with reports of increased geopolitical and military tension between India and China (Source: Recorded Future)

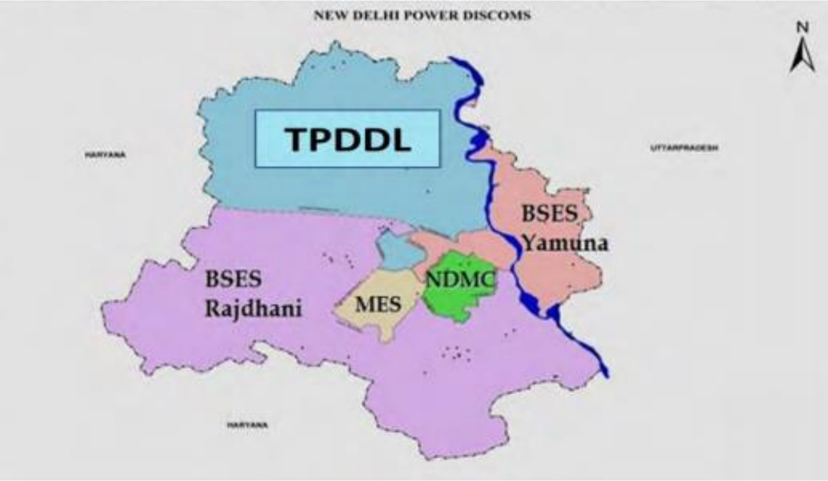
Some the major cyber attacks that were carried out on Indian soil by China linked Threat Action Group (TAG in RecordedFuture terminology) RedEcho in October 2020, and China-linked TAG-38 in few months up to April 2022. Both of these campaigns were also heavily focused on the power sector, and have been covered below as CASE STUDY #1 and CASE STUDY #2. [8][9]

Below we can see all CI that was attacked in these two campaigns, notably Delhi SLDC was the only SLDC targeted in both the campaigns though none were able to disrupt supply, but lead to serious concerns regarding pre-positioning attacks. [8][9]


China
Pakistan
Nepal
Bhutan
Bangladesh
India
Myanmar (Burma)
Arabian Sea
Bay of Bengal
Delhi State Load Despatch Centre
DTL Tikri Kalan Substation
Mumbai Port Trust
Western Regional Load Despatch Centre
NTPC Kudgi STPP Power Plant
Southern Regional Load Despatch Centre
V. O. Chidambaranar Port
Telangana State Load Despatch Centre
Eastern Regional Load Despatch Centre
North Eastern Regional Load Despatch Centre
Port
Load Despatch Centre
Power Plant
Sub Station



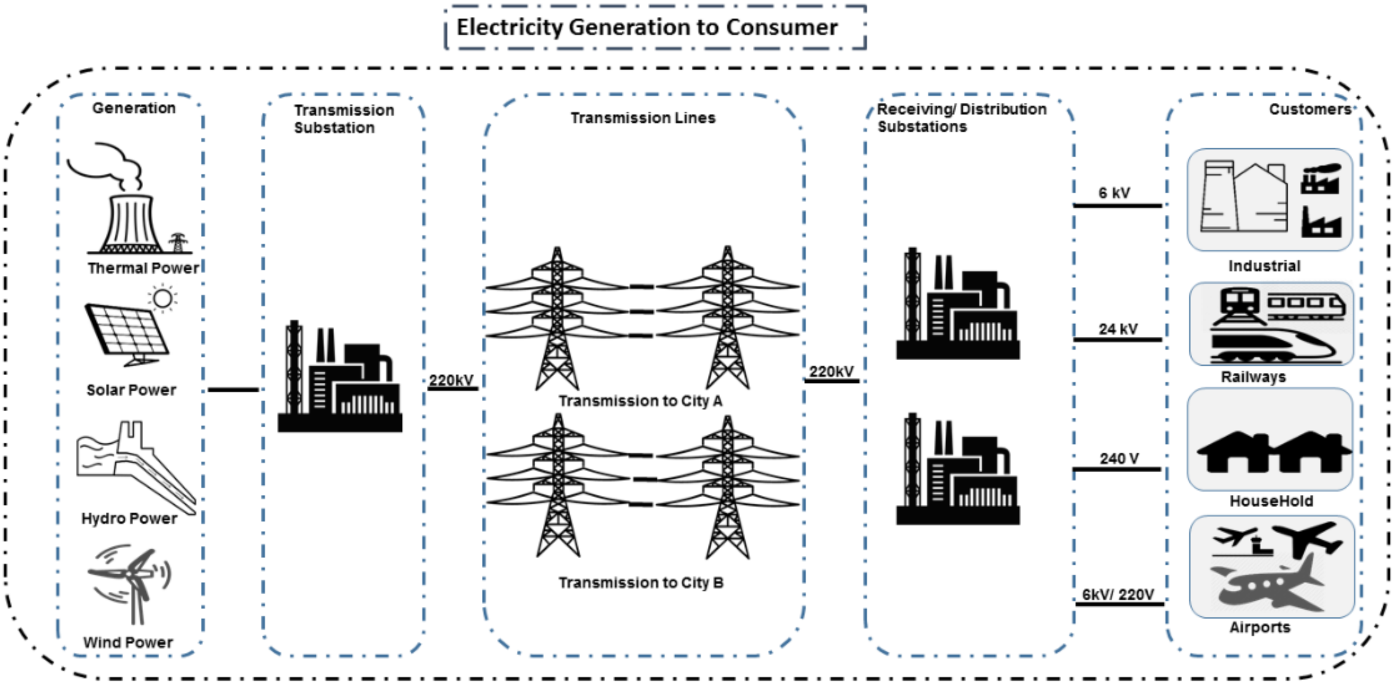
Now, Delhi SLDC is a rather lucrative target for any cyber-attack campaign because it houses NDMC and MES DISCOM (Distribution Companies) areas. These areas contain within them centers of Civil Power and Military Power respectively. This certainly explains why these are still under government DISCOMs, when all other areas were handed over to private players with 51% stake and government with 49% stake as back as 2002.[10][11]



After having learnt of NDMC and MES retention with government DISCOMs owning to their sensitive nature, it's safe to conclude any attack on these would be a threat to national security. So, this was my motivation to choose the defense of Delhi SLDC.

ARCHITECTURAL ASSUMPTIONS ON DELHI SLDC

Historically, power grids have grown from simple, localized grids to large, physically wide-spread grids, often spanning multiple nations or even whole continents. Increasing volatilities within power transmission and distribution force power grid operators to amplify their use of communication infrastructure to monitor and control their grid.[12]



Overview of a Modern Grid

All electricity that is generated must be used simultaneously, hence to make use of different peak hours and seasonal peaks thereby better utilizing the electrical power output. Therefore, a *"National Grid"* was established under known as Unified Load Dispatch and Communication (ULDC) Scheme [13], under which we have a hierarchical architecture as shown below.[14]

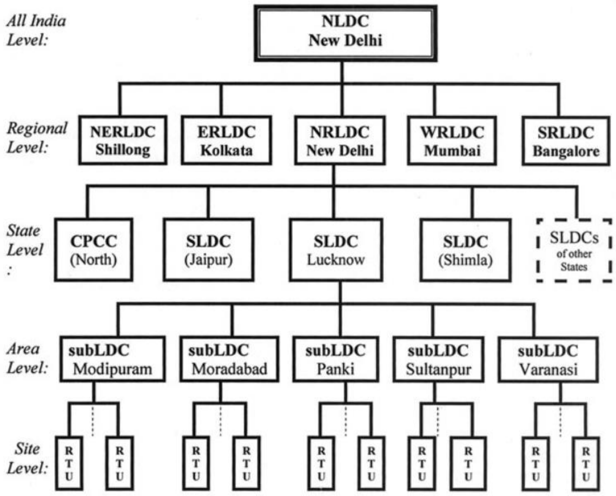
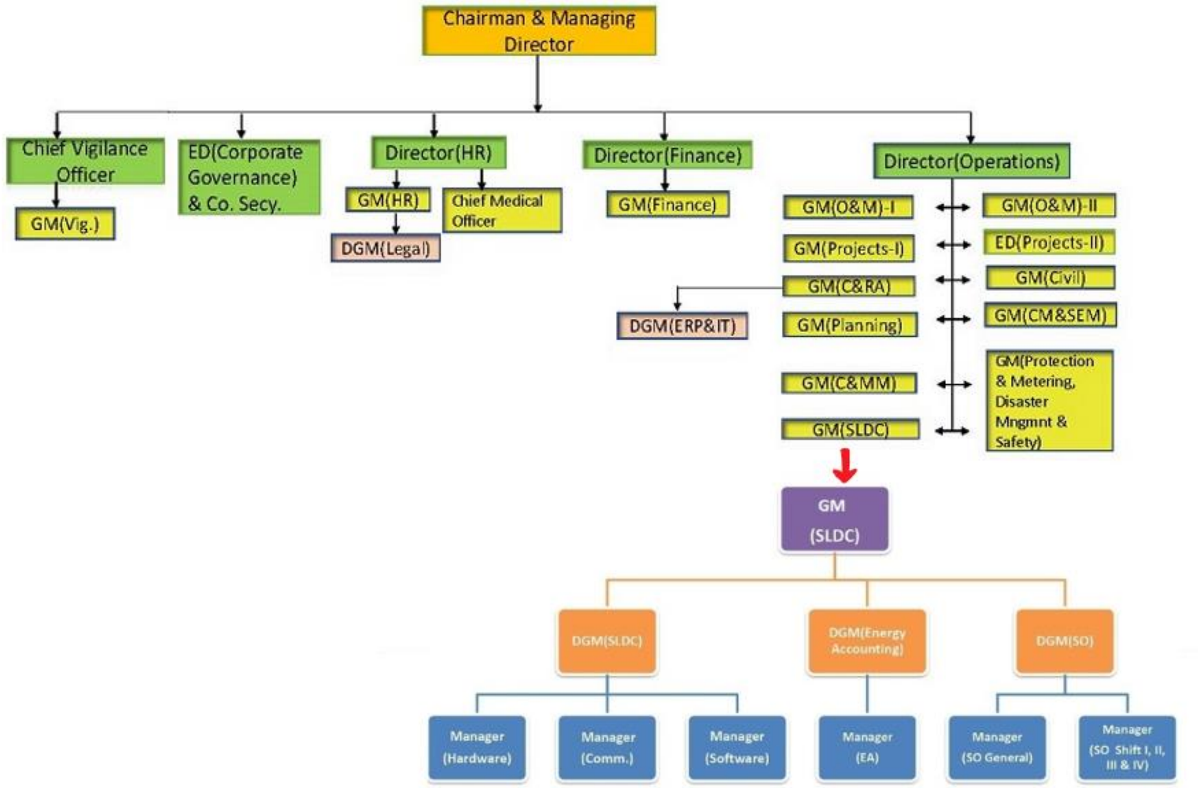


Figure 1: *Hierarchical Structure of Power System Control Centres*

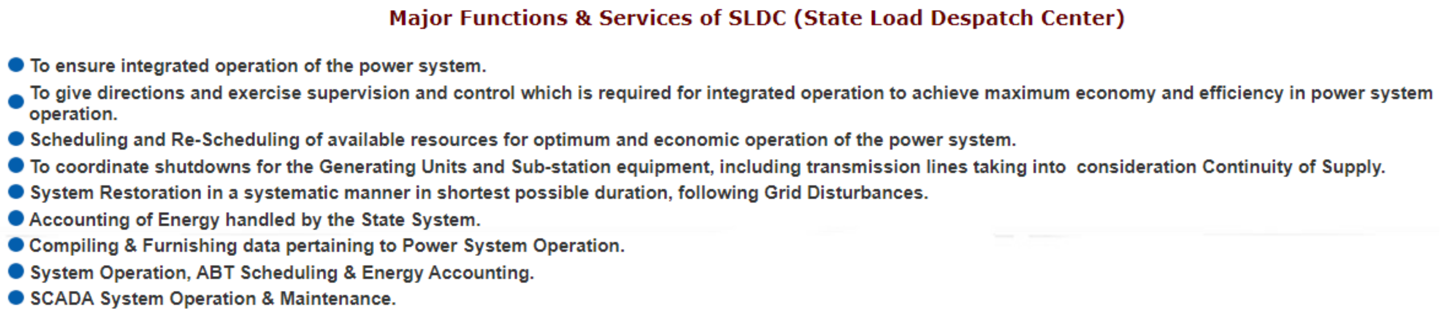
National Load Dispatch Center (NLDC) coordinates the activities of all RLDCs. NLDC, RLDCs, SLDCs and Sub-LDCs have their own SCADA systems, integrated in a hierarchical structure.

RLDC being at the top of hierarchy at regional level, coordinates the day-to-day operation of a region in consultation with SLDCs.

Now, since our target infra is Delhi SLDC which is run by Delhi Transco Limited, we will look at its organizational structure.[15] [16]



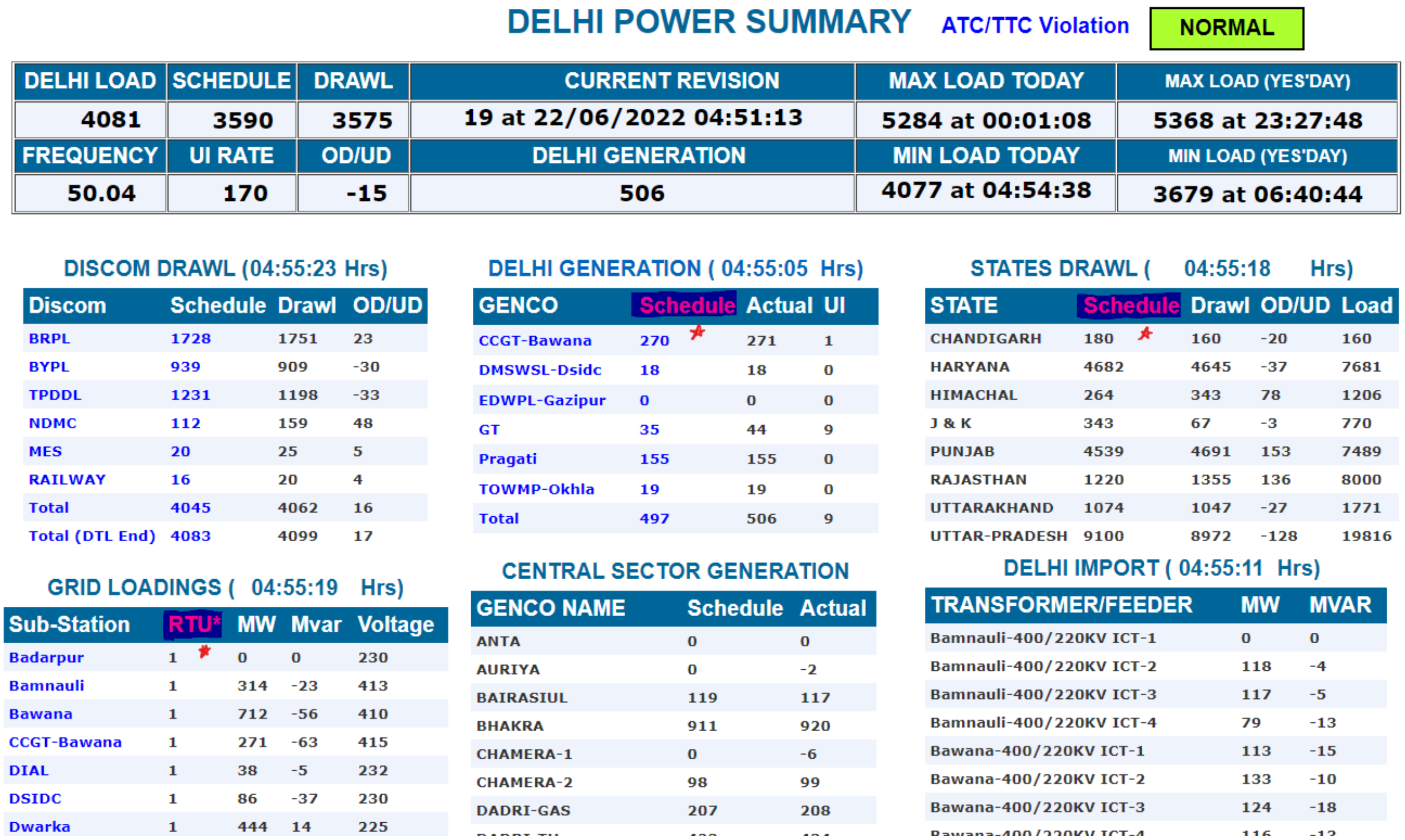
Delhi SLDC is the apex body to ensure integrated operations of power systems in Delhi, it was constituted under **Electricity Act 2003**, and its functions are shown below: [16]



Major Functions & Services of SLDC (State Load Despatch Center)

- To ensure integrated operation of the power system.
- To give directions and exercise supervision and control which is required for integrated operation to achieve maximum economy and efficiency in power system operation.
- Scheduling and Re-Scheduling of available resources for optimum and economic operation of the power system.
- To coordinate shutdowns for the Generating Units and Sub-station equipment, including transmission lines taking into consideration Continuity of Supply.
- System Restoration in a systematic manner in shortest possible duration, following Grid Disturbances.
- Accounting of Energy handled by the State System.
- Compiling & Furnishing data pertaining to Power System Operation.
- System Operation, ABT Scheduling & Energy Accounting.
- SCADA System Operation & Maintenance.

One of the most important tasks to perform is scheduling power output and instruct GENCOs (Generation Companies) on daily basis with predictions for 96 sectors (each 15 minutes).



DELHI POWER SUMMARY ATC/TTC Violation NORMAL

DELHI LOAD	SCHEDULE	DRAWL	CURRENT REVISION	MAX LOAD TODAY	MAX LOAD (YES'DAY)
4081	3590	3575	19 at 22/06/2022 04:51:13	5284 at 00:01:08	5368 at 23:27:48
FREQUENCY	UI RATE	OD/UD	DELHI GENERATION	MIN LOAD TODAY	MIN LOAD (YES'DAY)
50.04	170	-15	506	4077 at 04:54:38	3679 at 06:40:44

DISCOM DRAWL (04:55:23 Hrs)

Discom	Schedule	Drawl	OD/UD
BRPL	1728	1751	23
BYPL	939	909	-30
TPDDL	1231	1198	-33
NDMC	112	159	48
MES	20	25	5
RAILWAY	16	20	4
Total	4045	4062	16
Total (DTL End)	4083	4099	17

DELHI GENERATION (04:55:05 Hrs)

GENCO	Schedule	Actual	UI
CCGT-Bawana	270	271	1
DMSWSL-Dsidc	18	18	0
EDWPL-Gazipur	0	0	0
GT	35	44	9
Pragati	155	155	0
TOWMP-Okhla	19	19	0
Total	497	506	9

STATES DRAWL (04:55:18 Hrs)

STATE	Schedule	Drawl	OD/UD	Load
CHANDIGARH	180	160	-20	160
HARYANA	4682	4645	-37	7681
HIMACHAL	264	343	78	1206
J & K	343	67	-3	770
PUNJAB	4539	4691	153	7489
RAJASTHAN	1220	1355	136	8000
UTTARAKHAND	1074	1047	-27	1771
UTTAR-PRADESH	9100	8972	-128	19816

GRID LOADINGS (04:55:19 Hrs)

Sub-Station	RTU*	MW	Mvar	Voltage
Badarpur	1	0	0	230
Bamnauli	1	314	-23	413
Bawana	1	712	-56	410
CCGT-Bawana	1	271	-63	415
DIAL	1	38	-5	232
DSIDC	1	86	-37	230
Dwarka	1	444	14	225

CENTRAL SECTOR GENERATION

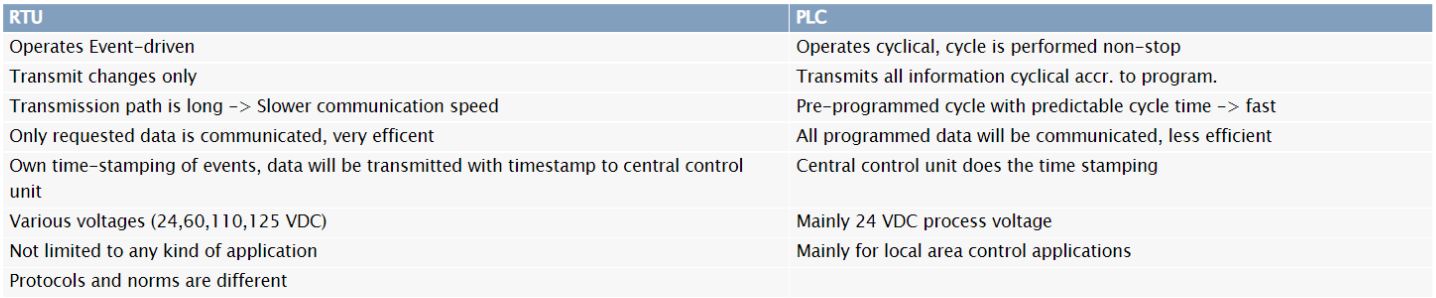
GENCO NAME	Schedule	Actual
ANTA	0	0
AURIYA	0	-2
BAIRASIUL	119	117
BHAKRA	911	920
CHAMERA-1	0	-6
CHAMERA-2	98	99
DADRI-GAS	207	208

DELHI IMPORT (04:55:11 Hrs)

TRANSFORMER/FEEDER	MW	MVAR
Bamnauli-400/220KV ICT-1	0	0
Bamnauli-400/220KV ICT-2	118	-4
Bamnauli-400/220KV ICT-3	117	-5
Bamnauli-400/220KV ICT-4	79	-13
Bawana-400/220KV ICT-1	113	-15
Bawana-400/220KV ICT-2	133	-10
Bawana-400/220KV ICT-3	124	-18

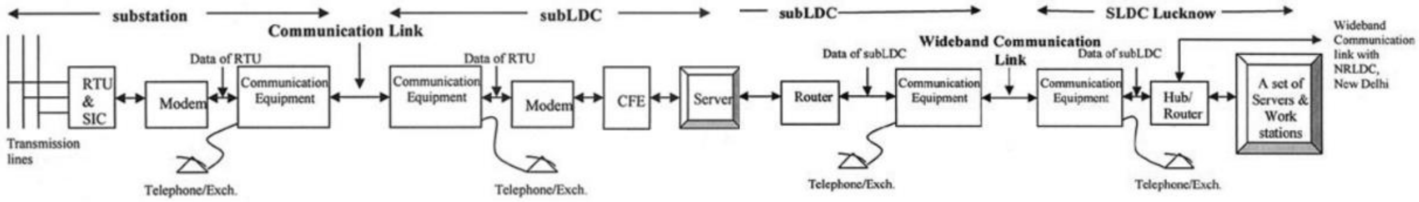
Electrical power grids rely on a stable grid frequency of 50 Hz due to the use of alternating current. The frequency is only stable if power generation and consumption are at an equilibrium. If more power is generated than consumed, the frequency rises, and vice versa. [12]

Now, to carry on such large arrays of responsibilities, **in general** the SLDC need constant input of data from the Remote Terminal Units (RTUs) in the sub stations. RTUs are microprocessor-based device that monitors and controls field devices, that then connects to plant control or SCADA (Supervisory Control and Data Acquisition) systems, these have many considerable advantages above PLCs and hence are more commonly used.



RTU	PLC
Operates Event-driven	Operates cyclical, cycle is performed non-stop
Transmit changes only	Transmits all information cyclical accr. to program.
Transmission path is long -> Slower communication speed	Pre-programmed cycle with predictable cycle time -> fast
Only requested data is communicated, very efficent	All programmed data will be communicated, less efficient
Own time-stamping of events, data will be transmitted with timestamp to central control unit	Central control unit does the time stamping
Various voltages (24,60,110,125 VDC)	Mainly 24 VDC process voltage
Not limited to any kind of application	Mainly for local area control applications
Protocols and norms are different	

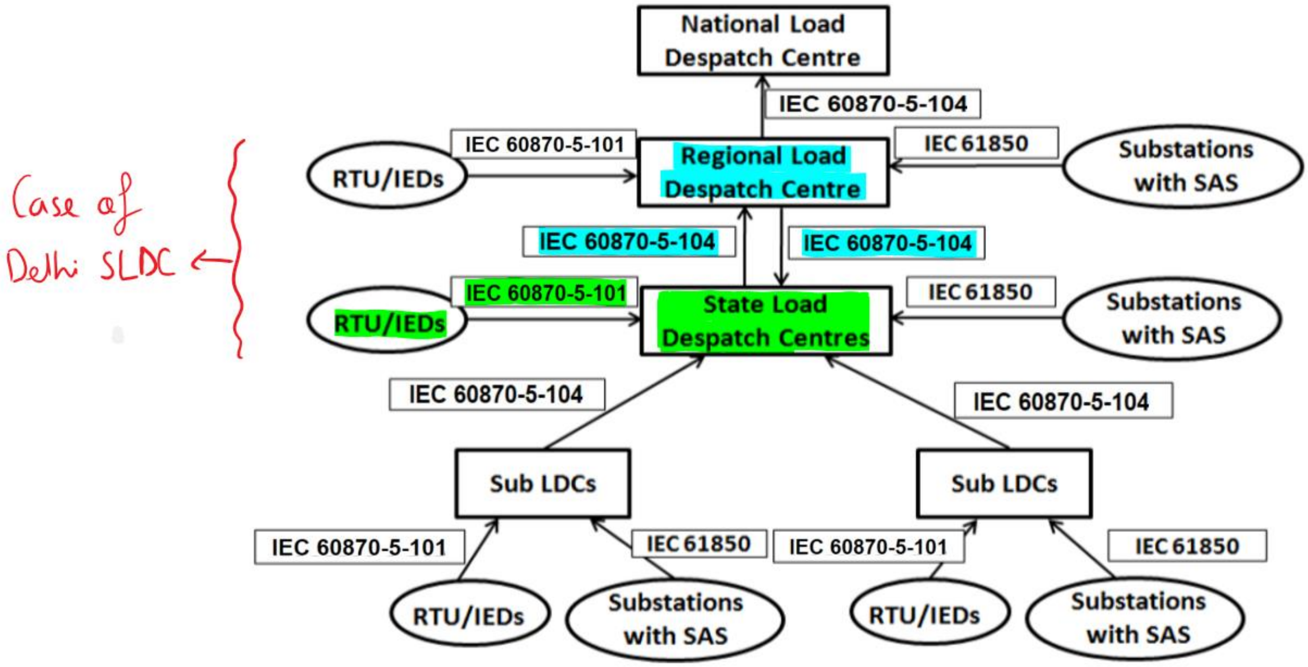
Now, so many RTUs interconnected with the SLDCs results in large SCADA network, which is visualized below (Assuming similar structure in NRLDC's region, hence using Lucknow SLDC documentation):



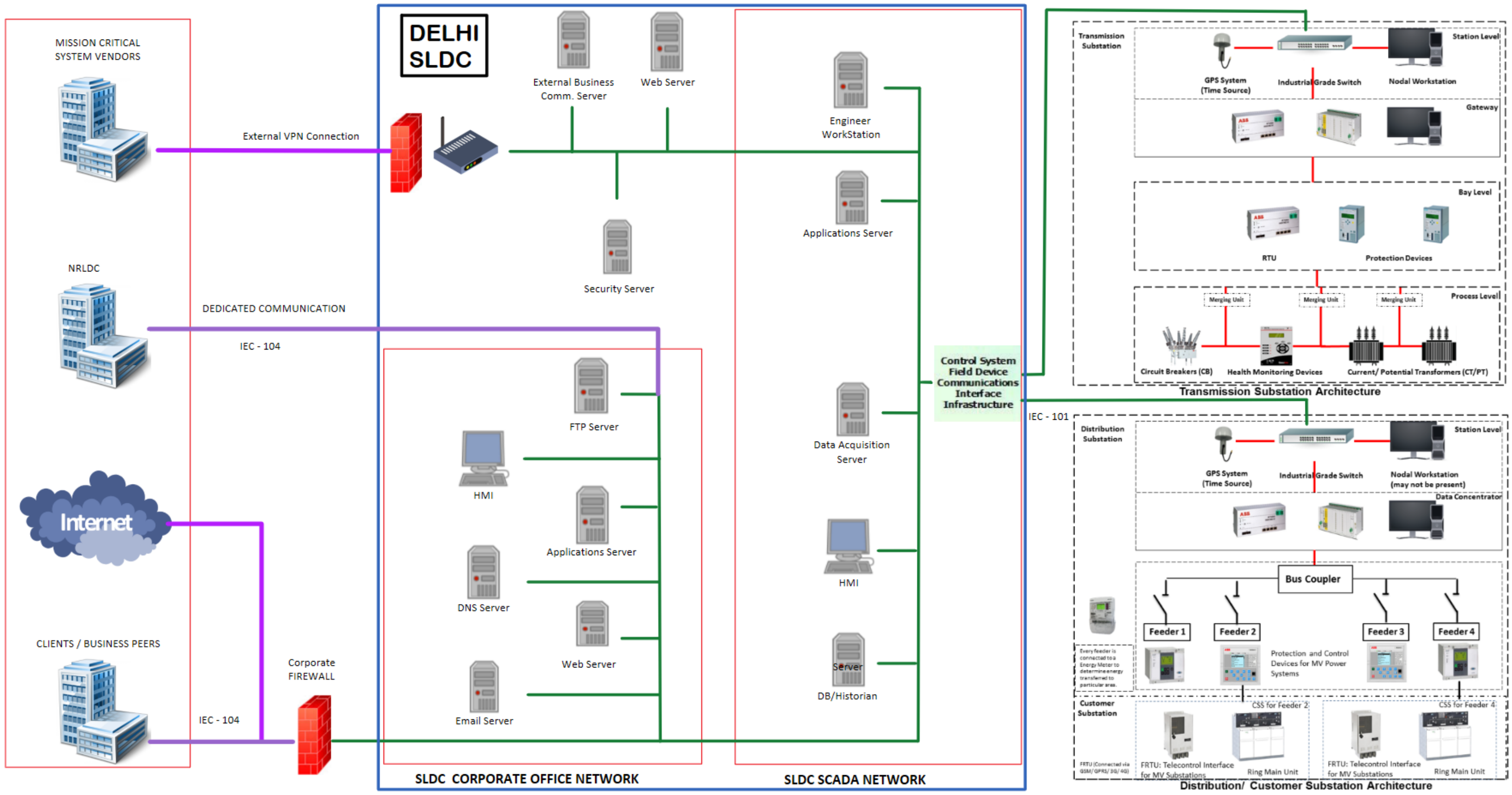
Source: https://upptcl.org/upptcl/en/article/power-system

Now, **in case of Delhi** due to small geographical area there is no need for sub-LDCs and there is direct communication between substation and SLDC. Presently, two-level of control hierarchy is being followed in DTL, where at the bottom are RTUs at the sub-stations and top level is SLDC as given on their official website. SLDC data in turn flows to NRLDC (Northern RLDC), POSOCO. All the regional Load Dispatch Centers are reporting to NLDC (National Load Dispatch Centre), to have Uniform grid operation at national level. [15]

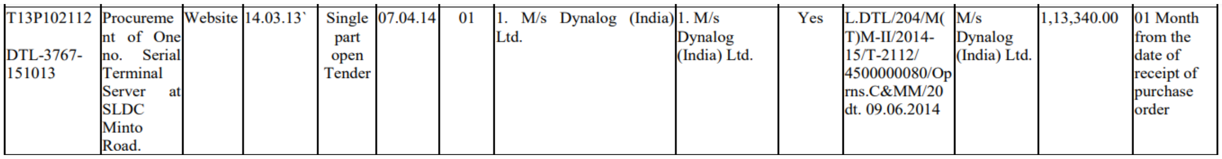
There is a lot of communication going on and the protocols used are listed below IEC 60870-5-104 (IEC - 104) and IEC 60870-5-101 (IEC - 101) is predominantly used [17]:



Based on sources (given) and some assumptions I have rendered an in-depth Architectural Diagram for communication between sub-stations (both distribution and transmission), SLDC and NRLDC is as shown below:



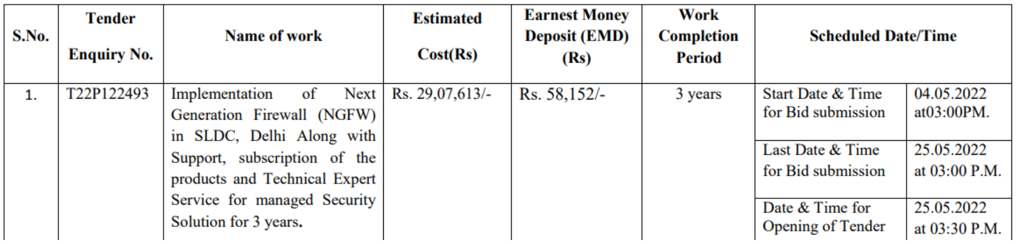
During my research I was also able to **verify** some aspects of above architecture (till now based on sources as mentioned), that is *while going through the tenders* that were floated by **Delhi Transco Limited**, I came across some *interesting* awarded tenders, along with the vendors shown below:



T13P102112 DTL-3767-151013	Procurement of One no. Serial Terminal Server at SLDC Minto Road.	Website	14.03.13`	Single part open Tender	07.04.14	01	1. M/s Dynalog (India) Ltd.	1. M/s Dynalog (India) Ltd.	Yes	L.DTL/204/M(T)M-II/2014-15/T-2112/ 4500000080/Oprns.C&MM/20 dt. 09.06.2014	M/s Dynalog (India) Ltd.	1,13,340.00	01 Month from the date of receipt of purchase order

Source: http://dtl.gov.in/WriteReadData/userfiles/file/Tenders%20Awarded_M-II%20CMM.pdf

Also, the awarded tender section has not been updated since **Last Updated On: 14 Sep 2017**, so I was not able to dig deeper into it, but in listing of new tenders I also found something interesting:

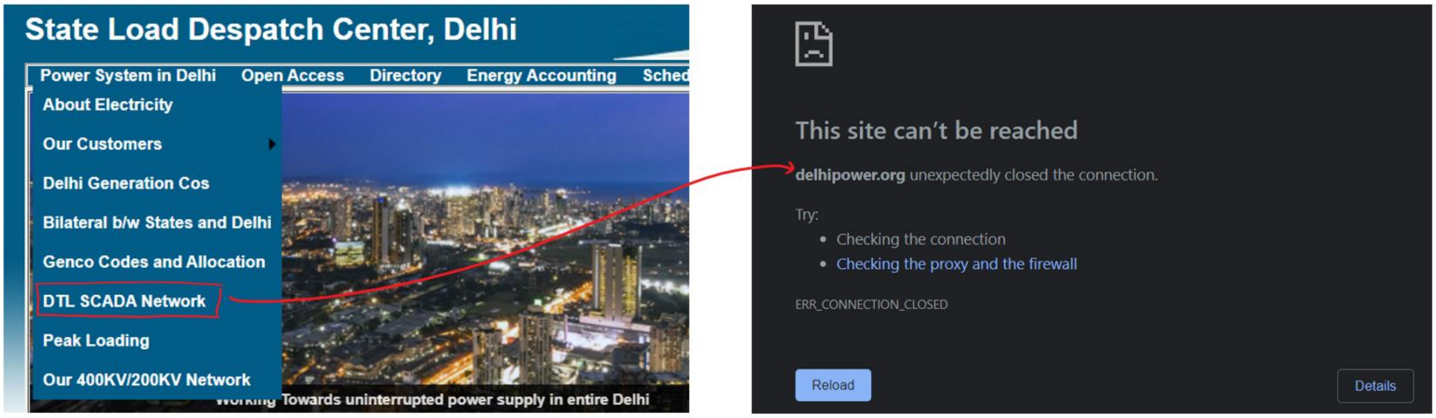


S.No.	Tender Enquiry No.	Name of work	Estimated Cost(Rs)	Earnest Money Deposit (EMD) (Rs)	Work Completion Period	Scheduled Date/Time	
1.	T22P122493	Implementation of Next Generation Firewall (NGFW) in SLDC, Delhi Along with Support, subscription of the products and Technical Expert Service for managed Security Solution for 3 years.	Rs. 29,07,613/-	Rs. 58,152/-	3 years	Start Date & Time for Bid submission	04.05.2022 at03:00PM.
						Last Date & Time for Bid submission	25.05.2022 at 03:00 P.M.
						Date & Time for Opening of Tender	25.05.2022 at 03:30 P.M.

Source: http://dtl.gov.in/content/49_1_CurrentTenders.aspx

Apparently, the SLDC has recently felt the need for **NGFW**, and a subscription to products and Technical Expert Services, this could have been a response to recent breaches by China using IoT devices based out of South Korea and Japan, as discussed in CASE STUDY #2 below.

Also, the VPN access assumption seems to be quite accurate because when I tried to access DTL SCADA Network link on https://www.delhisldc.org/, I wasn't able to access it:



This site can't be reached

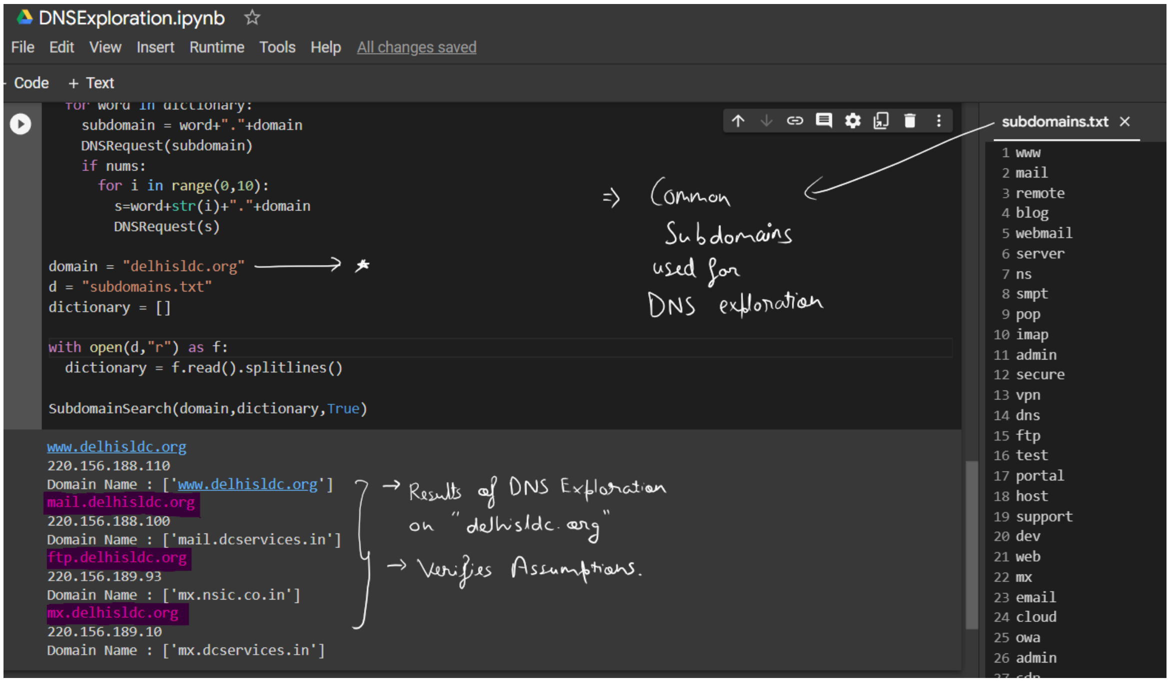
delhipower.org unexpectedly closed the connection.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_CLOSED

I also ran a DNS Exploration for 'delhisldc.org' (GitHub Link) so as to test out my theories using a python script, which immediately confirmed the existence of many servers as listed below (here subdomain.txt is a text file containing some common subdomain names)



```
  for word in dictionary:
    subdomain = word+"."+domain
    DNSRequest(subdomain)
    if nums:
      for i in range(0,10):
        s=word+str(i)+"."+domain
        DNSRequest(s)

domain = "delhisldc.org"
d = "subdomains.txt"
dictionary = []

with open(d,"r") as f:
  dictionary = f.read().splitlines()

SubdomainSearch(domain,dictionary,True)
```

```
www.delhisldc.org
220.156.188.110
Domain Name : ['www.delhisldc.org']
mail.delhisldc.org
220.156.188.100
Domain Name : ['mail.dcservices.in']
ftp.delhisldc.org
220.156.189.93
Domain Name : ['mx.nsic.co.in']
mx.delhisldc.org
220.156.189.10
Domain Name : ['mx.dcservices.in']
```

```
www
mail
remote
blog
webmail
server
ns
smpt
pop
imap
admin
secure
vpn
dns
ftp
test
portal
host
support
dev
web
mx
email
cloud
owa
admin
```

⇒ Common Subdomains used for DNS exploration

→ Results of DNS Exploration on "delhisldc.org"

→ Verifies Assumptions.

POSSIBLE ATTACK Vectors/Methodologies:

With such complex structures and resulting increase in communication creates a large surface for malicious actors. Now there are many attack vectors both Traditional and Specific, and we will talk briefly about those in context of this case:

I) Some Traditional Attack Vectors are:

- Sniffing/spoofing attacks – IEC 60870-5 (both -101 and -104) do have built-in data authentication capabilities (credibility and integrity) as shown below, but lack data encryption techniques, even for sensitive data like important instructions, etc. All data is transmitted in the clear and hence susceptible to MiTM attacks, DoS, social engineering campaigns etc.

- Lateral Movement of Malware – Attacks like that on Ukrainian Power Grid have shown that office networks (connected to the Internet) are often not sufficiently separated from the SCADA network, allowing attackers lateral movement between the two. Once an attacker gains access to an unsecured SCADA network, simple tools enabling communication in the specific protocol may be used to control devices crucial for grid operation.

- Remote Maintenance Access - Manufacturers of control room software and hardware usually have a maintenance contract with the grid operators using their systems and are equipped with some form of remote maintenance access to be able to debug these systems remotely or to deploy software updates, this is also a potential attack vector for the attackers and if a vulnerability is found, an attack could have a considerable impact at multiple operators.

- Physical Access to SCADA network/RTUs – This allows attackers to insert infected USB drives and is of grave concern as now it can work its way laterally of vertically depending on the goals.

- Insider risks – This is one of the gravest concerns, especially in regards to Advanced Persistent Threats (APTs).

- Security debt/ Unpatched Common Vulnerabilities and Exposures (CVEs) - Security debt occur when we are still using outdated legacy systems with little or no cyber-security capabilities, and config logs have not been regularly updated. Also, unpatched CVEs published on legitimate platforms or illegitimate platforms are bound to be used.

- Zero-days – Now zero-days vulnerabilities are prized by attackers and is a very formidable attack vector.

II) Some Specific Attack Vectors are:

- Distributed Generation – According to new Solar Policy, individual households can now feed their excess solar energy into the grid. Naturally, the hardware and software use by individuals to operate power generation are often not as secure as it should be or

CASE STUDY #1

RecordedFuture, October 2020:

After deadly clash in the Galwan Valley, there was a noticeable increase in the provisioning of PlugX (heavily used by China-nexus groups) malware C2 infrastructure, much of which was subsequently used in intrusion activity targeting Indian organizations.

10 distinct Indian power sector organizations were including 4 of the 5 RLDCs responsible for operation of the power grid through balancing electricity supply and demand, have been identified as targets in attacks by Chinese TAG (Threat Action Group) RedEcho.

A subset of the RedEcho AXIOMATICASYMPTOTE servers were configured with domains spoofing various Indian power generation and electricity transmission entities. For example, the ntpc-co[.]com domain is likely a typosquat of ntpc[.]co[.]in, the website of Indian power generation company NTPC Limited.

An even larger proportion of the RedEcho-targeted Indian IP addresses were observed communicating with 2 AXIOMATICASYMPTOTE servers hosting a large number of DDNS domains (91.204.224[.]14 and 91.204.225[.]216). This included overlaps with APT41/Barium activity previously reported by Microsoft, such as the domain bguha.serveuser[.]com [8] misconfigured. Assuming a vulnerability in a large number of, solar installations is found, attackers may control the power fed into the grid and using Cascading Effects can bring down grid.

- BlackIoT – IoT botnet of high wattage devices–such as air conditioners and heaters give a unique ability to attacker to launch large-scale coordinated attacks on the power grid to cause disruption and hence cascading. For ex, many factories simultaneously attacked and shut down or many central AC simultaneously shut down could cause over surge in frequency and potentially outage.

- Weakest Link Scenario - Pick a vendor for the grid systems and try to compromise it and receive particulars and credentials and spoof authorization, and move up the supply chain to attack the grid.

POSSIBLE ATTACK Scenarios/ Methodologies:

Predicting the exact path any nation-state funded weapon-grade malware will take is not feasible, but attackers can leverage different attack vectors to reach certain scenarios and cause damage and disruption:

- Disconnecting Resources – One of the basic scenarios is when certain entities are disconnected from the main grid to create disruptions, potentially before kinetic action.

- Injecting False Information – Injecting false information at the feeder level or at the SCADA network level can have serious implications as grid operators are not able to correct any deviations from 50Hz frequency or are forcefully deviating due to wrong info, and both are extremely dangerous scenarios. [18]

- DoS and DDoS attacks – DoS and DDoS attacks affecting the billing capabilities of DISCOMs to bill the energy which they supply as in the case of Colonial Pipeline Ransomware attack, that is their IT (Information Technology) is compromised but OT (Operation Technology) is still functional, but refused to pump gas as it was would have been a loss making venture.

- Cascading Effects - The sensitive equilibrium between generation and consumption can be exploited by attackers, as they only need to control a comparably small amount of consumption or generation to use cascading effects within the grid to create a system-wide blackout. For ex, in case of decreased grid frequency multiple cities have to be disconnected from the grid or power plants have to be downregulated to save the GE from damage.

CASE STUDY #2

RecordedFuture, April 2021:

Report by RecordedFuture observed likely network intrusions targeting at least 7 SLDCs. Notably, this targeting has been geographically concentrated, in proximity to the disputed India-China border in Ladakh.

One of these SLDCs was Delhi SLDC, only SLDC to be targeted in both campaigns.

To achieve this, the group likely compromised and coopted internet-facing DVR/IP camera devices for command and control (C2) of Shadowpad malware infections, as well as use of the open-source tool FRP, FastRecoverProxy. And the victim's infrastructure was observed communicating to all of the identified ShadowPad C2 servers, which had typo-squatted domain names of many Indian energy companies.

Though no evidence of ICS access was found. FRP can read predefined configurations and allows you to expose local services that are hidden behind the NAT or a firewall to the internet.

This might have been a Based on the complexity present across national critical infrastructure systems, this often necessitates lengthy reconnaissance operations to better understand the inner workings of these systems, both in a technological and a physical sense. [9]

CYBER DETERRENCE CHALLENGES

I. **Difficult to attribute an attack to a Nation** → It's really difficult if not impossible to trace an attack to a nation-state with concrete, undeniable evidence, as they have already taken many precautionary measures to maintain deniability.

II. **Cyber-warfare can cause huge damage on both sides** → As with kinetic war, now-a-days the stakes of a full-blown cyber-war have also increased as much of a nation's economy relies on Critical Infrastructure, therefore a good assessment of weaknesses and probable escalation should be kept in mind before a counter cyber-attack.

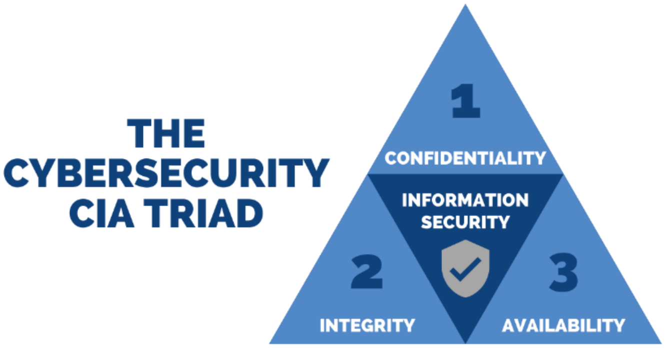
III. **Uncertainty regarding pre-positioning attack** → Cyber-operations continue to provide countries with a potent asymmetric capability to conduct espionage or pre-position within networks of hostile state for potentially disruptive reasons.

IV. **Diversionary Tactics** → Cyber-attacks can also be used to cause diversions before a kinetic attack so that much of command's attention in military outpost like Ladakh is glued to the cyber-incident.

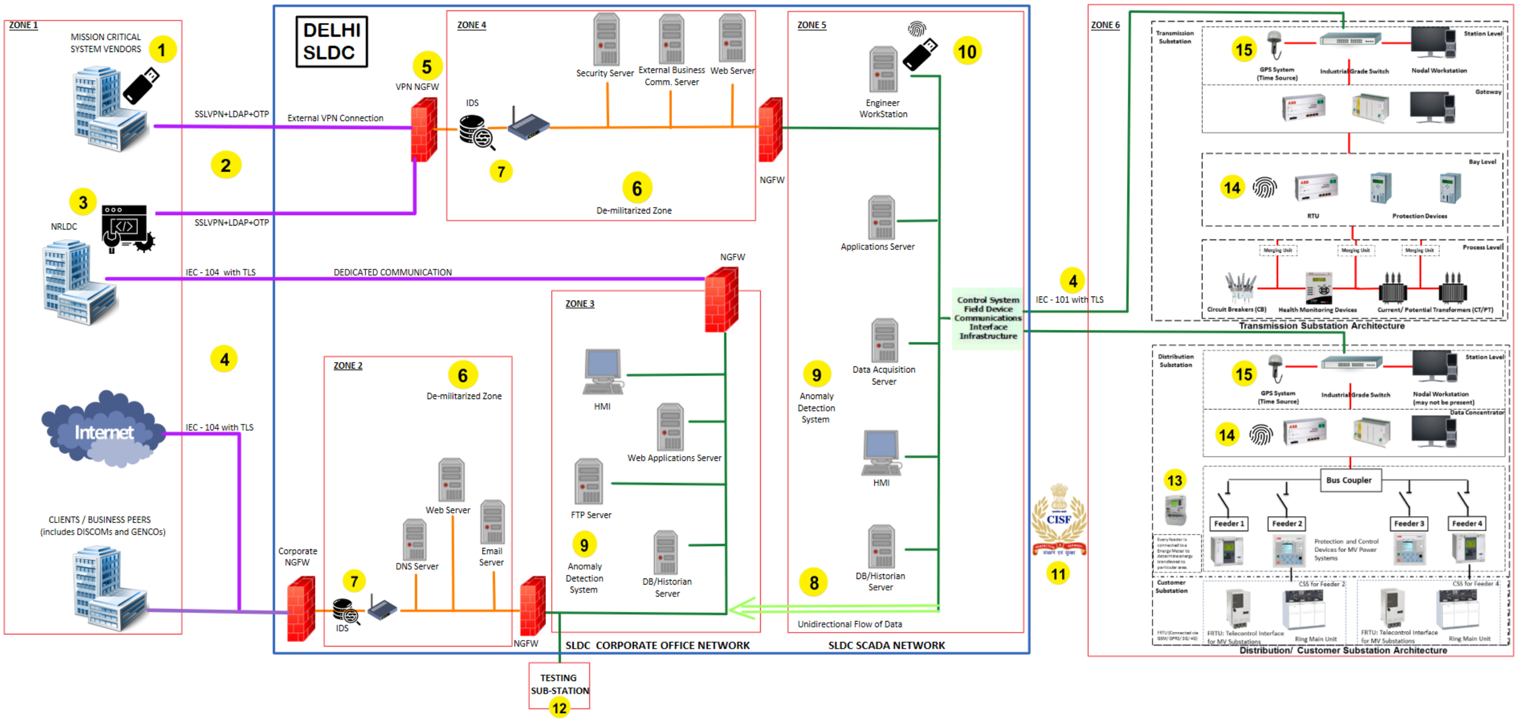
V. **Arms-Race Tactics** → Continued cyber-attacks can also be used to drain an economically-weak nation, if a nation has to spend lots of money to keep its C.I. safe, the nation is being forced to spend like Soviet-American arms race during the Cold War, which will lead to institutions failing.

SOLUTION ARCHITECTURE

Given the tremendous threats resulting from the diverse set of attack vectors and scenarios, providing security for power transmission and distribution within the grid as a critical infrastructure is a paramount objective.



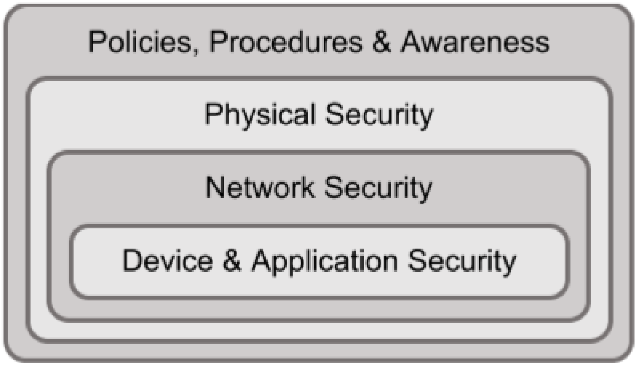
So, in compliance with the cyber security triad – CIA [12], in electric grid, however, availability is by far the most important measure of the triad as the consequences of downtime can be severe, the longer a blackout lasts and the more of the grid is affected, the harder it is to rebuild the grid. Any measures ensuring the confidentiality and integrity of systems should never interfere with the availability of power delivery. Below **I have rendered the proposed Solution Architecture for Delhi SLDC** along with markers for further references.



Note: For a clearer view at the Solution Architecture (Shortened to fit in this sheet), Parent OneNote File Submitted as a Supporting Doc

Please have a look at the OneNote File for better understanding of this proposed Solution Architecture

The proposed solution follows a **Zonal Architecture**, separate functionalities and access privileges based on zones of operation (as shown in the above architecture). Also, following the principle of Defense-in-depth, providing security for interconnected power grids needs to encompass a comprehensive set of measures, divided into 4 aspects. [12]


Policies, Procedures & Awareness
Physical Security
Network Security
Device & Application Security

DEVICE AND APPLICATION SECURITY

- **Key USB-sticks** – This device issued to mission critical system vendors **(No. 1)** will act as a key to allow connections to be made to the VPN firewall. It will *record sessions timing and user sessions*, and is used as a deterrent against insider threats that want to disrupt operations. Similarly, for SCADA network inside

SLDC the workstation engineer will be provided with Biometric-based USB **(No. 10)**, which will allow the person to operate on Engineer workstation, also Autorun scripts are to be turned off for all purposes.

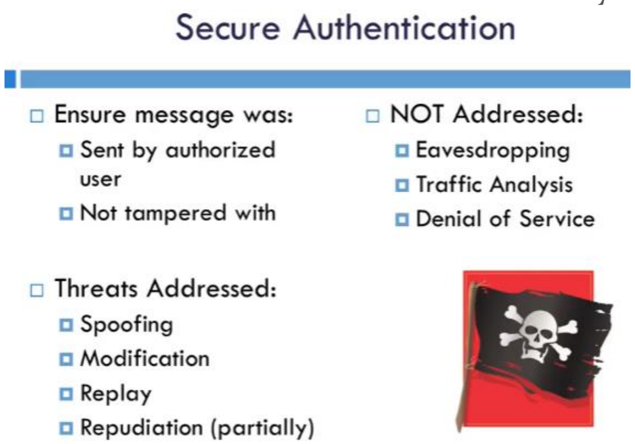
- **Physics-based ASIC Feeder** – Now, physics-based solutions are always a better alternative where frequent changes are not required. This can also be upgraded to ASIC components, as they are completely secure. **(No. 13)**

- **Proprietary Software** – **(No. 3)** This will be used by the NRLDC to send in secure commands through SSLVPN connection, and has a dedicated communication channel to SLDC with listen-only mode, this one over IEC-104 + TLS (Encryption also implemented).

NETWORK SECURITY

- **VPN connection with three-factor authentication** – VPN is established **(No. 2)** over SSL and has LDAP credential requirements managed by dedicated Authentication server, also since only Vendors with USB stick and NRLDC with proprietary software are allowed to connect that too with OTP at beginning of their session.

- **Using TLS over IEC 60870-5 (-101 and -104)** – We discussed various protocols used in SCADA communication above, though **(No. 4)** IEC 60870-5 (-101 and -104) can be trusted for secure authentication but they don't apply encryption and hence are susceptible to DoS, eavesdropping, etc., so we can use TLS over it to avoid such attacks. This is a classic case of security debt.



Secure Authentication

□ Ensure message was:
- Sent by authorized user
- Not tampered with

□ NOT Addressed:
- Eavesdropping
- Traffic Analysis
- Denial of Service

□ Threats Addressed:
- Spoofing
- Modification
- Replay
- Repudiation (partially)

Source: Triangle MicroWorks (communication Protocol Development organization)

- **Next-Generation Firewalls** – As already seen above in DTL issued tenders, NGFW **(No. 5)** have been chosen as they are ***stateful, rules-based and application-level*** firewall with ability to filter content because they can examine entire network packets.

- **Demilitarized Zones** – DMZs **(No. 6)** make it harder for attackers to get a comprehensive view of the network through simple reconnaissance methods (As happened in *CASE STUDY #2*) and restrict lateral movement within the network. [19]

- **Intrusion Detection System** – A *distributed IDS* **(No. 7)** for the power grid combines network-based and host-based IDS and centrally aggregates and correlates data provided by the systems distributed within the network. Such a distributed IDS allows a more complete view on the traffic within, also IDS have been chosen over Intrusion Prevention Systems (IPSs) as they automatically block potentially suspicious activity therefore should be restricted to non-safety-critical communication.

- **Unidirectional Flow of Data** - (**No. 8**) This ensures that no data can be sent to SCADA network (ZONE 5) from Office network (ZONE 6), thereby effectively acting as an air-gap while still transmitting all the data from DB/Historian server of SCADA network to DB/Historian Server of Office network so that this can be made available to DISCOMs and GENCOs, this also indirectly creates data backup.

- **Anomaly detection system** – This system (**No. 9**) can detect anomalies in a network and raise an alarm when required. Also, it's one of the best tools to combat insider risks, this learns, and keeps a track on usage and type, and compares it with the colleagues with similar privileges, this helps in pre-empting an insider risk, which can be then be monitored.

PHYSICAL SECURITY

- **Physical security at the SLDC (CISF)** - (**No. 11**)

- **Biometric Access to Energy Meters** – These systems (**No. 13**) are crucial to proper functioning of grid as they measure the electricity flowing through the feeder lines for distribution.

- **Biometric Access to RTUs** – These systems (**No. 14**) are present in all sub-stations act as the main SCADA networks there and send all info to Delhi SLDC.

POLICIES, PROCEDURES AND AWARENESS

- **No external USB stick policy, Autorun switched off policy** - (**No. 15**) This policy ensures no surprises at lower-level SCADA networks at substation and that SLDCs can trust the metrics being sent.

- **Central authority to Certify and Distribute** – There is a need for Central Authority to certify outside Vendor parts that are critical for operation are SLDC's Cybersecurity complaint and certify existing vendor's patches as safe for operational use, it will also maintain the proprietary software to be used by NRLDC.

- **Procedures for Zero-day exploits/Incident Response** – It's important to have procedures in place for zero-day exploits and a repeatable, dependable system to be in place. An incident response procedure will instruct employees on the steps to take if a computer on the network has been compromised. All employees should be trained on, and have access to, the procedure before an incident occurs. The questions to be covered in a contingency plan like:

    1. What are the indications that an incident has occurred or is currently in progress?
    2. What immediate actions should be taken (e.g., should the computer be unplugged from the network)?
    3. Who should be notified, and in what order?
    4. How should forensic evidence be preserved (e.g., should the computer be left on to preserve the evidence in memory)?
    5. How can the affected computers be restored?

- **Security Debt and CVEs remediation** - Resolution of core security problems almost always require updating, upgrading, or patching the software vulnerability or removing the vulnerable application. Also employee config should be updated regularly. And as the software hole can reside in any of the three layers (networking, operating system, or application). Whenever a CVE mitigation is available, it should be provided by the vendor or developer for the administrators to apply.

- **"Operation crossroads"** – Under this it is proposed that we make a small fake-grid complete with SCADA network in place and maintain its operations outside ZONE 5 with direct connection to SLDC's office network, to study all parameters so if an undetected attack happens, we can study this setup.

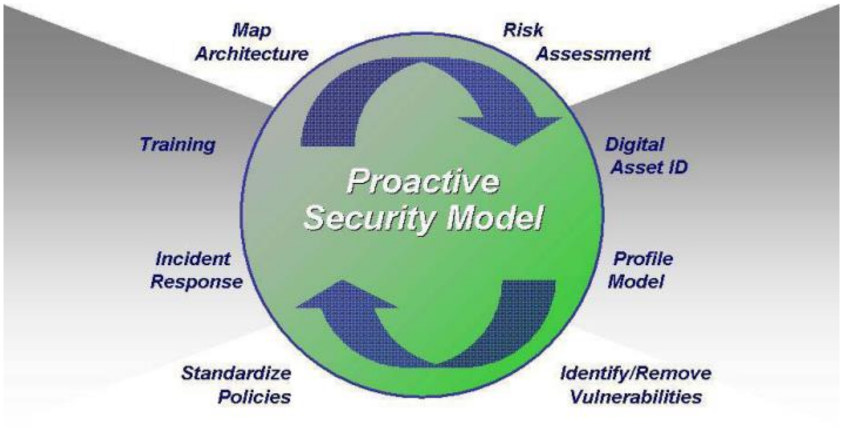
- **Constant surveillance of dark net** – This is to get to know what all vulnerabilities are being sold in the market; this is a similar case to that of Xiang Li.

- **Collaboration with Academia** – Collaborate with academia (Researchers, Ph.Ds., etc.) to produce better physics-based ASIC alternative to existing network-based solutions, and fund relevant researches in Institutes of National Importance. Its because physics-based ASIC components are good alternatives if the problem of high-frequency control can be solved

- **Security awareness program for employees** – Aware employees are less susceptible to Social engineering attacks like phishing, etc.

- **Bounty-hunting programs** – These might deliver critical zero-day vulnerabilities before a malicious attacker can take advantage of them.

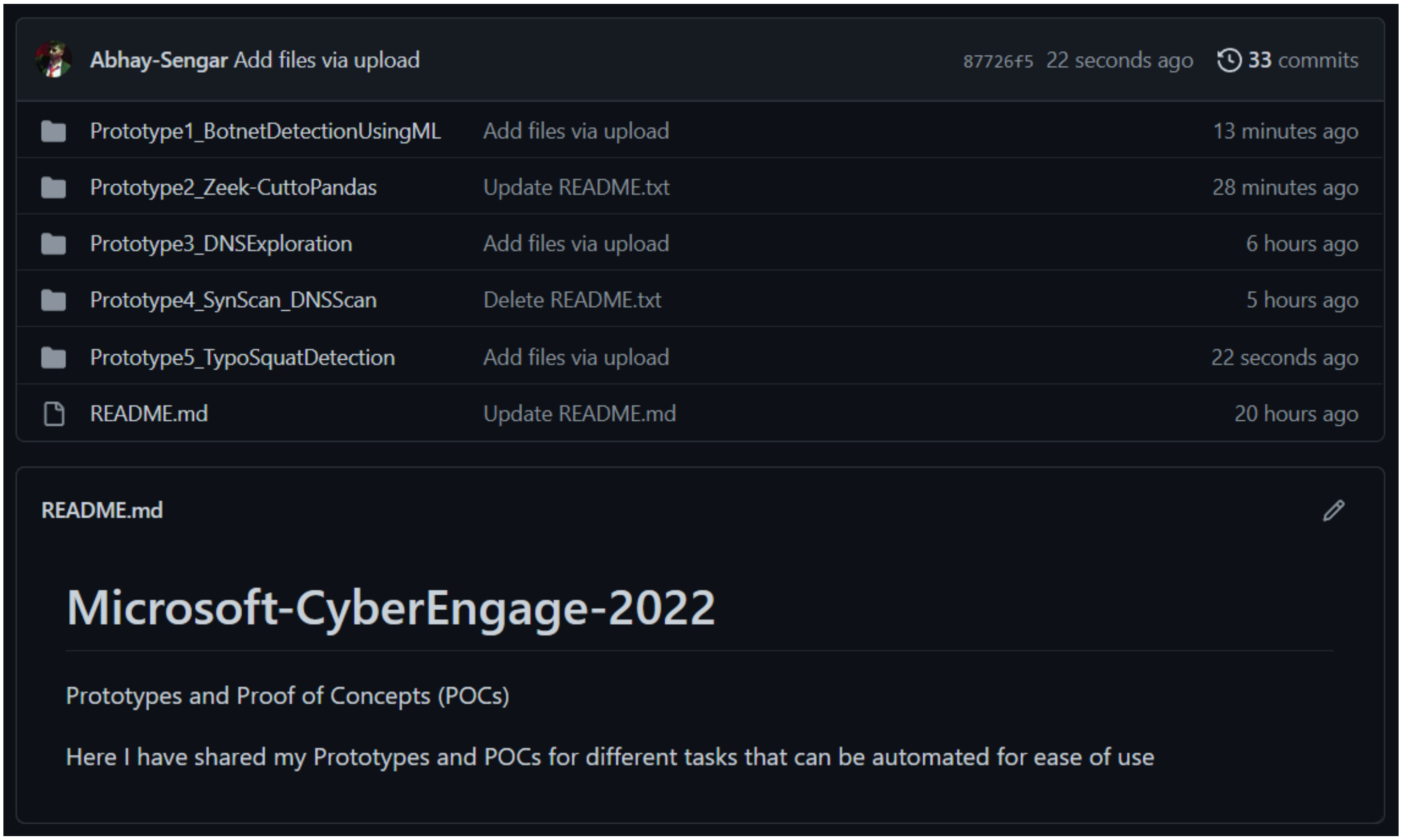
The above proposed solution architecture follows **Proactive Security model** [18], which is summarized below:



SOME INITIAL PROTOTYPES

This is the GitHub Repository for the prototypes developed: https://github.com/Abhay-Sengar/Microsoft-CyberEngage-2022

Its Highly Recommended to watch the Walkthrough as it covers the intent behind the prototypes



Abhay-Sengar Add files via upload 87726f5 22 seconds ago 33 commits

Prototype1_BotnetDetectionUsingML	Add files via upload	13 minutes ago
Prototype2_Zeek-CuttoPandas	Update README.txt	28 minutes ago
Prototype3_DNSExploration	Add files via upload	6 hours ago
Prototype4_SynScan_DNSScan	Delete README.txt	5 hours ago
Prototype5_TypoSquatDetection	Add files via upload	22 seconds ago
README.md	Update README.md	20 hours ago

README.md

Microsoft-CyberEngage-2022

Prototypes and Proof of Concepts (POCs)

Here I have shared my Prototypes and POCs for different tasks that can be automated for ease of use

I. **Botnet detection using ML** → Here I have trained a Decision Tree Classifier on a large dataset. All details are inside "Report.pdf" in the folder of Prototype 1, along with references used for mounting the dataset.

II. **Accessing Apache logs using Regex and Pandas** → This is to remove dependence on Zeek-Cut and allow to access data in Pandas DataFrame which has many built in functionalities that can be leveraged to write a better or improved Zeek-Cut utility.

III. **DNS Exploration** → The screenshot from above is from this script itself, also discussed during course.

IV. **Basic Syn Scan and DNS Scan performed** – This is also a tool used for reconnaissance, discussed during course.

V. **Typosquat Detection performed for 1 frequently used domain name** – Used dnstwist library to do a typosquat search for active domain name and then used code of Prototype 2 code for accessing all referrers from the apache logs (*Knowingly edited to show working of code*), and raise alarm.

BENCHMARKS FOR SUCCESS

I. **Relative Stability** → One of the benchmarks of success is that how did perform in overall availability with respect to other SLDC, as we have seen that there is a pattern of how multiple SLDCs have been targeted by the Chinese state actors as reported by RecordedFuture.

II. **Response to Zero-Day exploits** → how well contingency plan worked. Even if zero-day exploit response was unsuccessful, were we able to retain power in NDMC and MES due to power islanding and even if we lost there how much time it took us to restore power

III. **Incident Response** → Attack was detected and how successfully did we stop lateral movement and privilege escalation

IV. **Reduction in Security Debt Crisis/ Unpatched CVEs** → Cyber-attacks can also be used to cause diversions before a kinetic attack so that much of command's attention in military outpost like Ladakh is glued to the cyber-incident.

V. **Determined the target and procedures in forensics** → Continued cyber-attacks can also be used to drain an economically-weak nation, if a nation has to spend lots of money to keep its C.I. safe, the nation is being forced to spend like Soviet-American arms race during the Cold War.

VI. **Different behavior in small-fake grid** → If at any point in time there was some issue in the **(No. 12)** Fake grid (completes with SCADA systems) which is connected with office directly as was previously the case. And our current grid faces no such issue then the solution architecture is a success.

VII. **Successfully determined origin** → Now, during the Forensics we were able to determine with complete incriminating evidence then required action can be taken with respect to Legal and Treaty Assumptions, as shown below.

VIII. **During Retaliation offensive, destroyed capabilities of attacker** → If we are granted permission for retaliatory offensive, then it would be important to destroy their capabilities like C2 servers and pre-positioned malware for further attacks.

LEGAL AND TREATY ASSUMPTIONS

Targeting of Indian critical infrastructure offers limited economic espionage opportunities, and even though cyber-activists, etc. may target G.o.I., they have no incentive to attack critical infrastructure, so when critical infrastructure is attacked its either state sponsored or an act of cyber-terrorism. Since, India is not signatory of **Budapest Convention on Cybercrime**, hence not entitled to request data on any cyber-incident from signatory host countries of threat actors. But, due to strong Indian Foreign policy and the geo-political climate in the world, we do have **48 Extradition treaties** (Source: https://mea.gov.in/leta.htm). Assuming we were able to determine the source of malicious activities against us, if source is:

Friendly/Neutral Nations

In this case, state sponsored attacks are not a likelihood so mostly it was an incident of cyber-terrorism and since almost every extradition treaty covers terrorism, a case can be made for these.

1. **Attacker(s) identified and enough evidence was gathered:**
    - We have an Extradition Treaty → We can try extradition of the attacker(s) since almost all extradition treaties have clause for terrorism, a case can be made for it. For ex, France, Maldives, etc.
    - We don't have an Extradition Treaty → Use the Interpol construct to reach out, and then launch a criminal case under the nation's laws.

2. **Only the host nation was determined:** Use the Interpol to initiate investigation, and also initiate Intel Sharing with the relevant authorities in the nation with competent authorities from India.

Hostile Nations

While dealing with non-friendly states its more likely to be state-sponsored as discussed above though cyber terrorism can't be ruled out, and they are not likely to co-operate even in face of mild international condemnation. However, things start to change if the nation is a known serial-offender with significant diplomatic pressure from many countries, as now there is fear of trade relations souring and restriction to markets of corresponding nations.

REFERENCES:

[1] Singer, Peter W. "Stuxnet and its hidden lessons on the ethics of cyberweapons." *Case W. Res. J. Int'l L.* 47 (2015): 79.

[2] Nourian, Arash, and Stuart Madnick. "A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet." *IEEE Transactions on Dependable and Secure Computing* 15.1 (2015): 2-13.

[3] Denning, Dorothy E. "Stuxnet: What has changed?." *Future Internet* 4.3 (2012): 672-687.

[4] Van Dine, Alexandra. "After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities."

[5] https://www.nec.com/en/global/insights/report/2020022506/index.html

[6] https://www.itu.int/en/ITU-D/RegionalPresence/AsiaPacific/Documents/Events/2020/CNI%202020/WK-ITU-CNI-Webinar-Philip.pdf

[7] https://csis-website-prod.s3.amazonaws.com/s3fs-public/220527_SignificantCyberIncidents.pdf?kBE7Y6AT0nePQxJbCxS8m98V2zdIqIj_

[8] RecordedFuture Report: "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions"

[9] RecordedFuture Report: "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group"

[10] https://www.timesnownews.com/india/article/delhi-govt-has-49-shareholding-in-power-discoms/1991

[11] https://www.uday.gov.in/images/Presentation%20by%20Tata%20Power.pdf

[12] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors*, *21*(18), 6225.

[13] Pradeep, Yemula & Medhekar, Abhiroop & Maheshwari, Piyush & Khaparde, S.A. & Joshi, Rushikesh. (2022). Role of Interoperability in the Indian Power Sector.

[14] https://upptcl.org/upptcl/en/article/power-system

[15] http://dtl.gov.in/

[16] https://www.delhisldc.org/HomeSldc.aspx

[17] Agrawal, V. K., et al. "Experience of integrated operation of SCADA/EMS system at national level—a case study." *2014 Eighteenth National Power Systems Conference (NPSC)*. IEEE, 2014.

[18] https://inldigitallibrary.inl.gov/sites/sti/sti/3375141.pdf

[19] "Protecting Critical Infrastructure Against the Next Stuxnet" Doug Nibbelink Davenport University CAPS 795 Dr. Lonnie Decker March 20, 2013

---- Remaining Links have already been provided in-text ----